WE CLAIM

1. A removable physical media bearing a computer program operable to control a computer to detecting malware by performing the steps of:

booting said computer with a non-installed operating system read from said removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files; and

performing malware detection upon said computer using said one or more malware detection files.

2. A removable physical media as claimed in claim 1, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

3. A removable physical media as claimed in claim 1, wherein said steps further comprise loading security management code operable to control said downloading.

4. A removable physical media as claimed in claim 1, wherein said steps further comprise establishing a secure network connection to said remote computer.

5. A removable physical media as claimed in 4, wherein a firewall computer disposed between said computer and said remote computer is operable to block a

connection between said computer and said remote computer other than said secure network connection.

6. A removable physical media as claimed in claim 1, wherein said non-installed operating system is a Windows PE operating system.

7. A removable physical media as claimed in claim 1, wherein said removable physical media is one of:

an optical disk;
a floppy disk;
a memory card; and
a removable disk drive.

8. A removable physical media as claimed in claim 1, wherein malware to be detected includes one or more of:

a computer virus;
a computer Trojan;
a computer worm;
a banned computer application;
a data file associated with a malware file; and
configuration settings of said computer associated with a malware file.

9. A method of detecting malware upon a computer said method comprising the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files; and

performing malware detection upon said computer using said one or more malware detection files.

10. A method as claimed in claim 9, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

11. A method as claimed in claim 9, comprising loading security management code operable to control said downloading.

12. A method as claimed in claim 9, comprising establishing a secure network connection to said remote computer.

13. A method as claimed in 12, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection.

14. A method as claimed in claim 9, wherein said non-installed operating system is a Windows PE operating system.

15. A method as claimed in claim 9, wherein said removable physical media is one of:

an optical disk;

a floppy disk;

a memory card; and

a removable disk drive.

16. A method as claimed in claim 9, wherein malware to be detected includes one or more of:

a computer virus;

a computer Trojan;

a computer worm;

a banned computer application;

a data file associated with a malware file; and

configuration settings of said computer associated with a malware file.

17. A computer operable to detect malware upon said computer by performing the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a remote computer one or more malware detection files; and

performing malware detection upon said computer using said one or more malware detection files.

18. A computer as claimed in claim 17, wherein said one or more malware detection files include at least one of:

malware definition data containing data characteristic of malware to be detected;

a malware detecting engine operable to control said computer to perform said malware detection;

a malware application shell; and

malware detection option settings operable to configure optional settings of said malware detection.

19. A computer as claimed in claim 17, wherein said steps further comprise loading security management code operable to control said downloading.

20. A computer as claimed in claim 17, wherein said steps further comprise establishing a secure network connection to said remote computer.

21. A computer as claimed in 20, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection.

22. A computer as claimed in claim 17, wherein said non-installed operating system is a Windows PE operating system.

23. A computer as claimed in claim 17, wherein said removable physical media is one of:

an optical disk;
a floppy disk;
a memory card; and
a removable disk drive.

24. A computer as claimed in claim 17, wherein malware to be detected includes one or more of:

a computer virus;
a computer Trojan;
a computer worm;
a banned computer application;
a data file associated with a malware file; and
configuration settings of said computer associated with a malware file.

25. A server computer connected by a network link to a computer detecting malware upon said computer by performing the steps of:

booting said computer with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer;

loading network support code for said computer read from said removable physical media;

downloading from a server computer one or more malware detection files; and performing malware detection upon said computer using said one or more malware detection files.